Business Use of Cryptography

Presented By: Jeffrey Roth
DSDC-TA
(614) 692-9898

Purpose

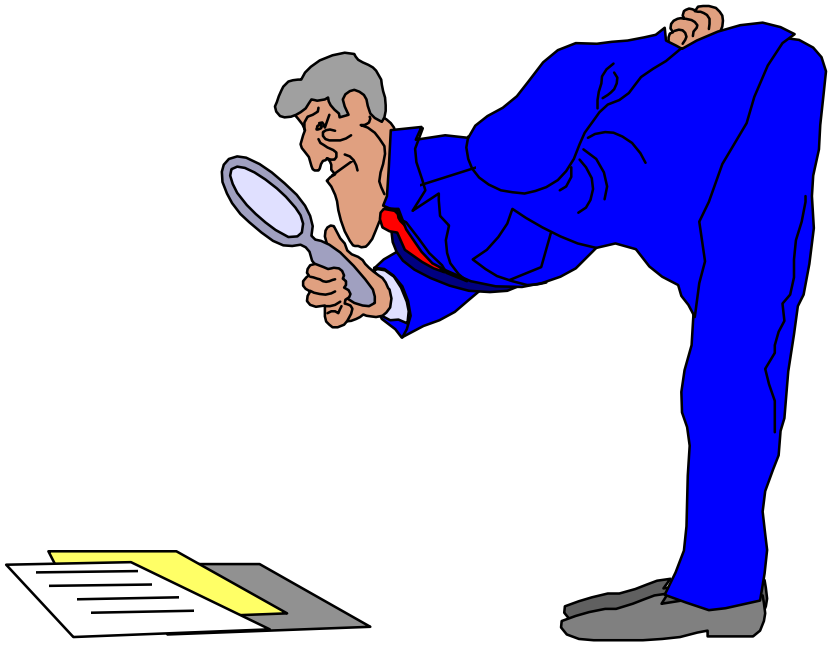
- Introduce Cryptographic Concepts
- Show Business Applications

Structure

- **Concepts**
- **Examples**
- **Applications**

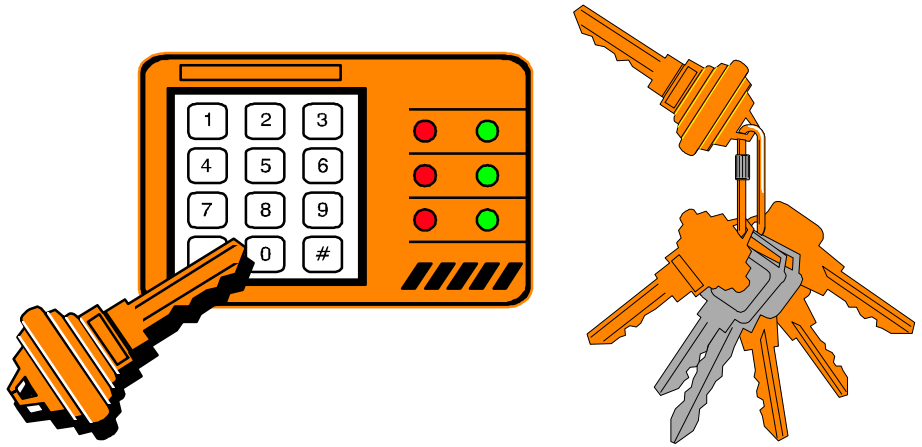
Crypto....

- Cryptography
- Cryptology
- Cryptanalysis



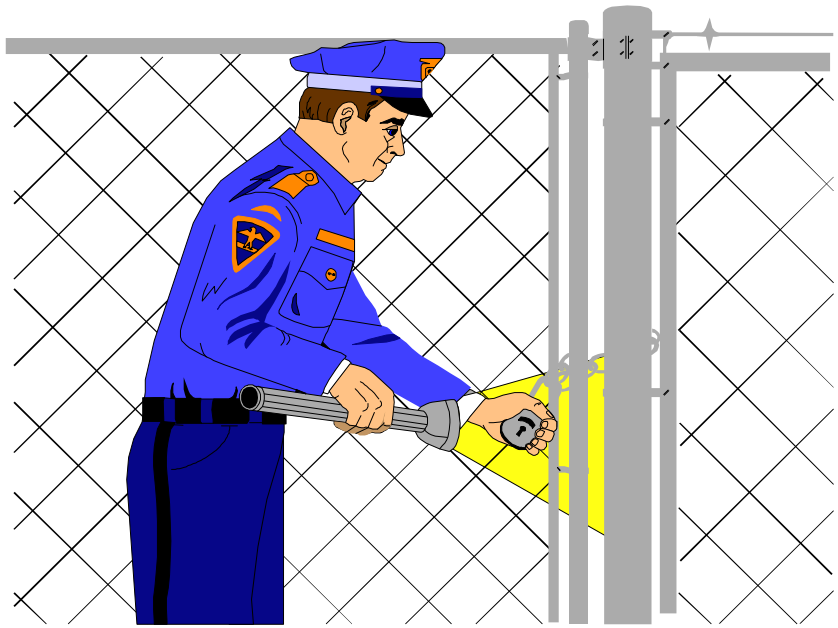
Concepts

- **Plaintext**
- **Ciphertext**
- **Algorithms**
- **Keys**



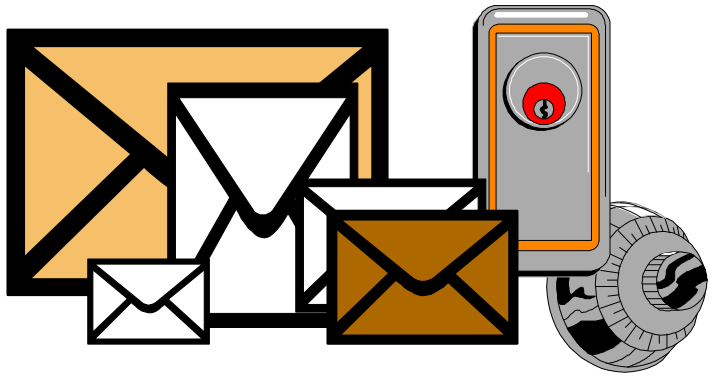
Security Terms

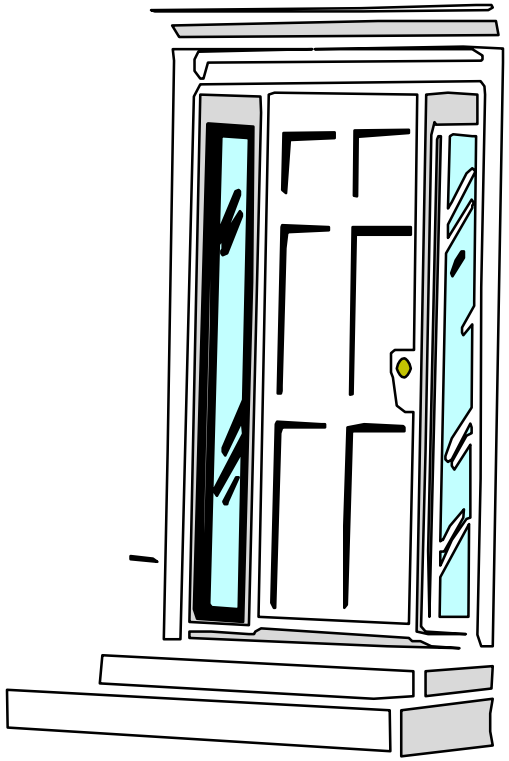
- **Authentication**
- **Integrity**
- **Privacy**



Business Practices

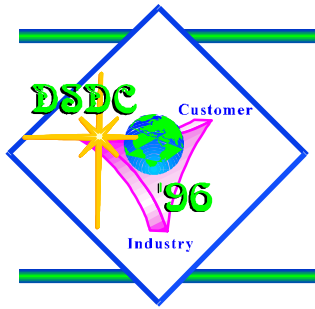
- Signatures, Badges, Passwords
- Envelopes, Locks, Seals
- Closed Doors





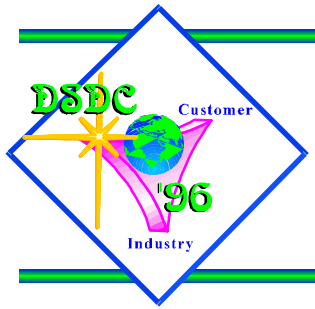
Cryptanalytic Techniques

- Known Text
- Educated Guessing
- Brute Force



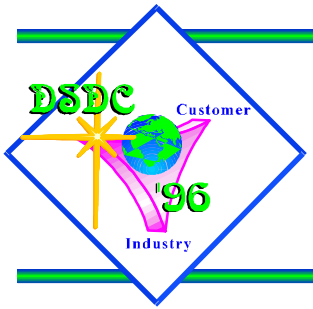
Low Grade Algorithms

- **Rot16**
- **UNIX Crypt Command**



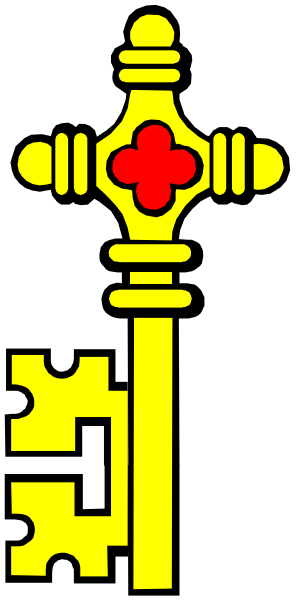
High Grade Algorithms

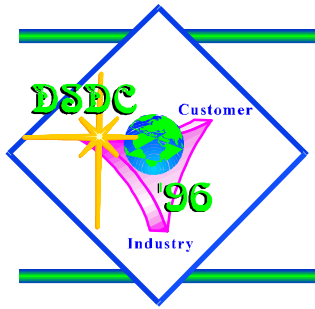
- DES
- IDEA
- RSA



Private Key Encryption

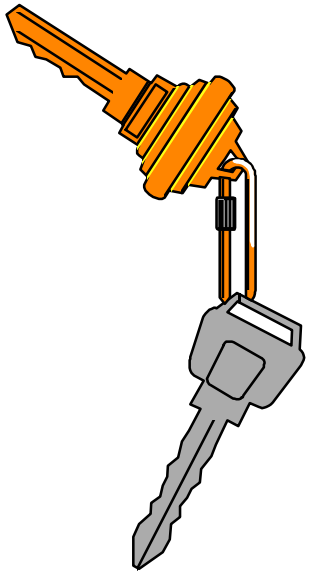
- Single Key to Encrypt/Decrypt
- Also Called Symmetric
- DES, IDEA

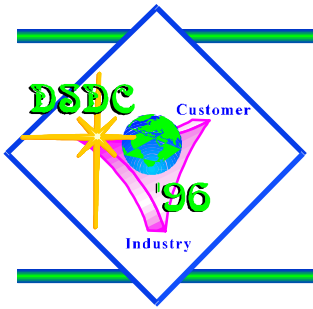




Public Key Encryption

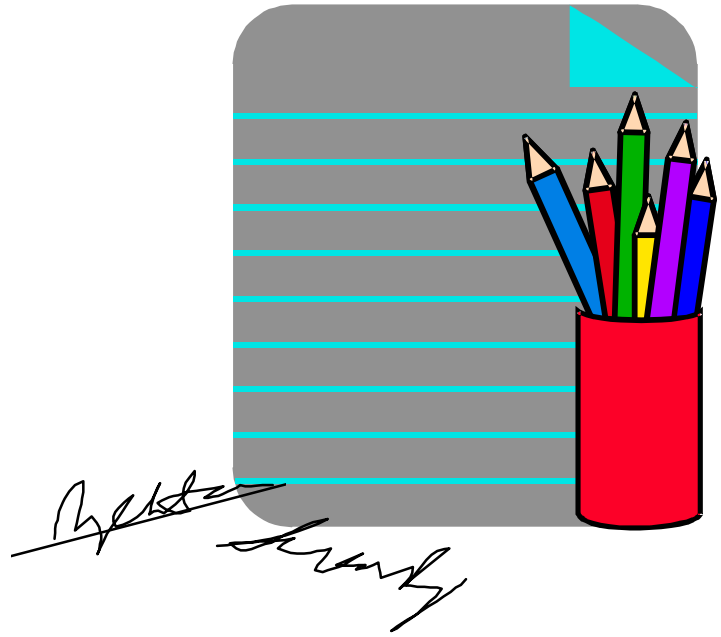
- Two Keys, One “Public”
- Can Encrypt or Sign
- RSA, Fortezza





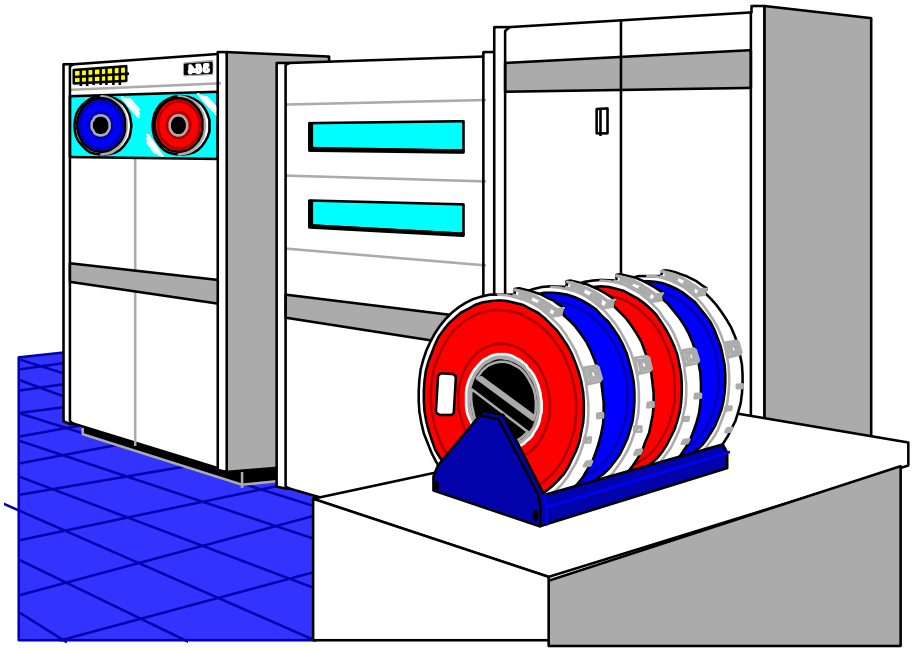
Applications

- **Passwords**
- **Single Signon**
- **Digital Signatures**
- **Message Digests**



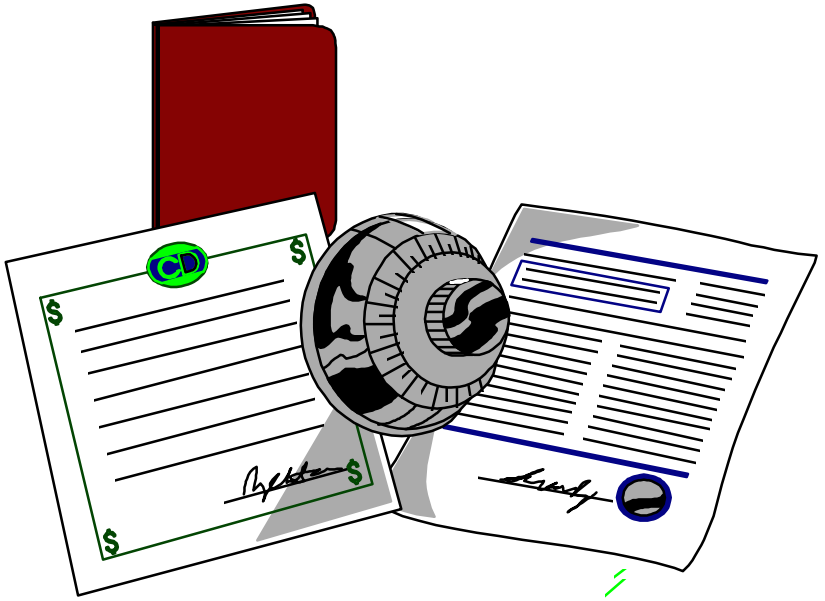
UNIX Passwords

- DES
- Hash, Not Password, Stored
- Vulnerabilities



Kerberos

- DES
- No Passwords On Net
- Trusted Third Party
- Vulnerabilities

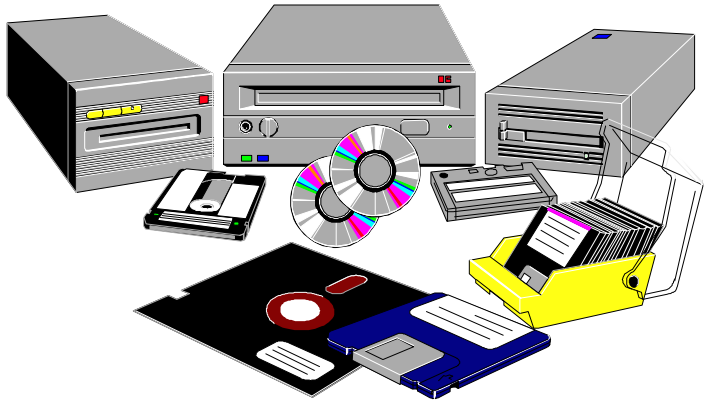


PGP

- RSA + IDEA
- Software Based
- Digital Signature + Encryption
- Online Public Key Distribution
- Chain of Trust

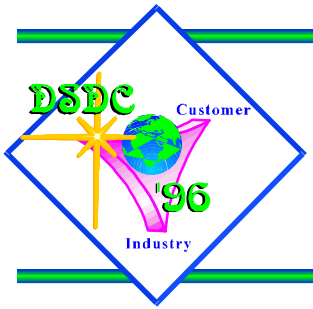
Fortezza

- Government Public Key Algorithm
- Hardware Based
- X.500 Public Key Distribution
- Key Escrow



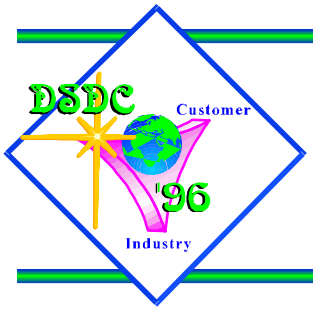
SSL

- Netscape, Other Web Servers
- End to End Encryption
- RSA
- Certificate Authority



Issues

- Implementation Errors
- The Human Element
- Export Restrictions
- Key Escrow



Questions and References

Business Use of Cryptography

Presented By: Jeffrey Roth
DSDC-TA
(614) 692-9898
Email: jroth@dsdc.dla.mil